Running head: Japanese OPSEC and the Hard-Worker

Japanese OPSEC and the Hard-Worker

MSG Minoru Koba

United States Army Sergeants Major Academy

SGM Rodolfo G. Garza

Class58

3 January 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 JAN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Japanese OPSEC and the Hard-Worker	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Sergeants Major Academy,11291 Sgt. E.Churchill St,Fort Bliss,TX,79918**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
In the Japanese Self Defense Force, Information leaks on the web through the file-sharing software infected by a computer worm happen one after another. Why did they use their privately owned computers in their work place? Why did they take their work home to do? The deterioration of Soldier?s moral on the Operational Security (OPSEC) and our working environment must have led to those incidents. I recommend that we lighten them and advocate how our ethics should be.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**7**	

Abstract

In the Japanese Self Defense Force, Information leaks on the web through the file-sharing software infected by a computer worm happen one after another. Why did they use their privately owned computers in their work place? Why did they take their work home to do? The deterioration of Soldier's moral on the Operational Security (OPSEC) and our working environment must have led to those incidents. I recommend that we lighten them and advocate how our ethics should be.

Introduction

In December 2002, an officer of the Infantry Regiment of the Japanese Ground Self-Defense Force (JGSDF) leaked sensitive files including members' address lists and drill plans of his regiment onto the internet. He stored the data on his privately owned computer (POC) and unwittingly uploaded the sensitive files on the Japanese file-sharing software Winny. Although the leaked files were unclassified, that was the first case that JGSDF leaked sensitive information onto the web via the Winny.

In February 2006, a Chief Petty Officer of the Maritime Self-Defense Force (MSDF) leaked confidential information via his POC onto the internet. The leaked information included personnel data on dozens of MSDF members, cipher-related documents, and documents on the planning of combat exercises. He used his POC for business and saved the confidential files in the local disk of the computer. He installed the Winny on his POC and the computer worm Antinny that causes information disclosure onto the web from an infected computer using the Winny, apparently infected on his POC. The leaked files included the Maritime Force's reports on training exercises conducted in Okinawa with U.S. Forces in 2005. After this case, information leaks on the web through the Winny, infected with the Antinny, happened one after another in many units in the Japanese Self-Defense Force. However, I don't think that only Winny and Antinny caused these cases. The deterioration of Soldier's moral on the Operational Security (OPSEC) and our working environment must have led to those incidents as well. In this paper, I will discuss them and how ethics should be advocated.

Winny and Antinny

Winny is a Japanese peer-to-peer (P2P) file-sharing software developed by Isamu Kaneko, who is a research assistant in computer engineering graduate course at the University of Tokyo. It takes its name from WinMx, which is also a freeware peer-to-peer

file sharing program and famous in United States. This software enable to find and get files of music, videos, and documents from the computers of other people. However, once you uploaded the information on Winny, no one can delete them.

Antinny is a computer worm which infects the computer through the web and uploads files in the computer onto the network of file-sharing software. Antinny works on uploading screenshots onto an image board and does the Denial-of-service attack to a copyright protecting agency web site.

Since the birth of the Winny in May 2002, Winny-shock has swept not only JGSDF, but also many Japanese authorities, such as Police Agency, Tax Agency, Insurance Companies, large enterprises, and major universities. Some new ridiculous user, who heard of Winny by the media, installed it and Antinny infected to his computer. Total file-leaking reported on mass media numbered 224 only in 2006. Although Winny itself is very useful if operated properly, Antinny cause unwilling uploads and deteriorates problem.

Background of Leaks

All personnel who caused the leak had something in common. Firstly, they all installed Winny in their POCs. Secondly, some of them used their POCs which installed Winny in their work place for businesses. Thirdly, some took their work home by using removable media. In theory, installing the Winny in our POCs for private use wouldn't be a problem. However, you shouldn't use Winny-installed POC for business. You shouldn't bring our POC into your work place for business use or take work home with you. These practices lead to mistreatment of sensitive information. Why did they use their POCs in their work place? Why did they take their work home with them? Could they have prevented the leaks?

Loosen OPSEC Awareness

The largest reason of those incidents is that many Soldiers of JGSDF didn't have vigilant security awareness. After the WWII, JGSDF was organized in 1951 to secure Japan from

adversaries while the US was fighting in the Korean Peninsula. The new national constitution renounces the right of war. The JGSDF has been working on combat training or disaster relief. Some have lost their awareness of how important information is. They have lost sight of how to manage information and how it affects our national security if it is leaked. Of course, we have been teaching OPSEC and the punishments for leaking information. This is taught during the Development Program, in all companies, or when we attended educational courses. However, it didn't fully cover the computer network security and couldn't catch up with recent progressive information technology.

Secondly, believe it or not, although Japan is a high-tech country, most of our military units didn't have enough government-owned computers for each individual. We had to supplement by using our POCs for work and JGSDF overlooked those situations due to the lack of funds in the budget. This problem affected Soldiers and the Japanese Government as well. They all may have lost sight of OPSEC awareness.

Japanese Hard-Worker

So, why did they have to take their work home? You may have heard that Japanese are hard-workers. Yes, it is true. The average desk works an average of 12-15 hours per day. Field workers, such as technicians and mechanics, work an average of 8 hours per day due to safety. In the Japanese work system, the headquarters and desk workers naturally become so busy and the workers always have to manipulate hours because they would rather be at home with their families. Some desk workers at times, take their backlog home by removable devices and work with them in the close environment to their family.

Most of vigilant workers who take their backlog home use stand-alone computers and don't save on a hard-disk. Only some careless workers work on their home computers, which are connected to the web and sometimes installed the file-sharing software.

Working hard is a beautiful thing. Japan rehabilitated the country from the ruins of WWII with their hard-work. But, working long is not good. It demands workers and their families stressful separations. We have to streamline work procedures and make it more effective without working long hours.

The Aftermath of Leaks

On February 2006, then Prime Minister, Junichiro Koizumi, ordered the Ministry of Defense (MOD) the special order for prevention of reoccurrence after the leak case of MSDF. MOD ordered all services not to use Winny on any computers including their POC. It also announced plans to purchase 56,000 government-owned computers for 40 million dollars so that all desk workers would no longer have to use their POC for work.

MOD changed the OPSEC regulations for prohibiting POC use in the work place and prohibited personnel from bringing out government-owned computers, even for temporary duty without permission. It also prohibited the use of privately owned removable media in the work place. Thus, we couldn't take backlogged work home.

However, the most important thing was to protect from leaking and to instill OPSEC awareness in all servicemen. OPSEC training is an NCO responsibility. Japanese NCOs must regret the consecutive leaks and execute appropriate OPSEC training for all servicemen.

Conclusion

On April 2007, Military Police arrested a MSDF Petty Officer for possessing the secret information of the US-developed Aegis Combat System classified as the US-Japan Special Secret without authorization. Although this incident didn't relate to Winny or Antinny, the leak of the secret information relating to US-Japan security, caused awareness to Japanese MOD.

Cyber warfare is a part of national security and the Global War on Terrorism. The leaks in Japan might threaten the security of the US, and Japan would lose the reliability in the

international society. Even though MOD creates perfect counter-policy for leaks, it doesn't work if all servicemen are not aware of it. We all have to fully understand it and take every effort to prevent leaks. The fundamentals for national security are that we understand OPSEC and maintain it in the work environment.